Jeffrey M Navon

From: Markus Jakobsson [markusj@research.bell-labs.com]
Sent: Friday, March 10, 2000 4:43 AM
To: jeffrey@cplplaw.com
Subject: comments

Jeff,

I have read your update on the spam patent application.
Some comments:

p 12 line 6 "one-time pad P" -> "using a stream cipher generated pad P"

p 15 l 16 "senders-specific" -> "sender and receiver specific"

claim 2: the address is not encrypted. Do you mean the MAC result? that can be sent as an extension to the email address that is peeled off by the gateway. You can also use special fields for additional info to transmit the MAC portion.

claim 3: again: no encrypted address. Do you mean later on that the message would also be encrypted, or do you refer to the MAC? Let's call the MAC result something like an "identifyer" to seperate it from standard encryption, and avoid confusion.

claim 4. not over a public key, but "using public key encryption"

figs after 120, the resulting email would be bounced. the sender would attach the "cost item" and send it again (this could be done automatically)
and when it comes again (no state needs to be kept by the recipient) then the recipent would handle it like a new incoming email.

also, 80, I am not sure what you mean here. is that out of band? normally you have to know the core address of the person you want to talk to.

Give me a call if you need to clarify and discuss.
Cheers,
Markus